Notice of Allowability

Application No. 09/885,427	**Applicant(s)** MADE, PETER A.J. VAN DER		
Examiner Russ Guill	**Art Unit** 2123		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an Amendment filed July 3, 2006*.

2. ☒ The allowed claim(s) is/are *11,13,14,17-23 and 26-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 7/30/2001, 3/29/2002 4/15/2002
   2/12/2003
   4/28/2003
   5/14/2003
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

REASONS FOR ALLOWANCE

1. The following is a statement of Examiner's reasons that the Applicant's invention defines over the prior art of record:

a. While Le Charlier ("Dynamic Detection and Classification of Computer Viruses Using General Behavior Patterns", 1995) and Custer ("Inside Windows NT", 1993) and Chi (U.S. Patent No. 5,978,917) teach a computer implemented method and a system for identifying malicious code in a target program, including automatically configuring the virtual machine to execute the target program, in one of three modes of operation based on the file format and the control fields within the header of the file, a first mode of operation comprising a real mode for executing programs comprising instructions based on DOS, a second mode of operation for executing target programs comprising a high level programming language, and a third mode of operation comprising a protected mode for executing target programs comprising thirty-two bit code; simulating values of the computer system with the one or more layered operating system shells of the virtual machine; setting behavior flags in order to track behavior of the target program in response to the simulated values, during execution of the target program by the virtual machine; storing a sequence in which the behavior flags are set in the register by the target program during execution of the target program by the virtual machine; passing behavior flag data and sequence flag data from the virtual machine to the computer system for evaluation after execution of the target program by the virtual machine; and evaluating the behavior flag data and sequence flag data with the computer system to determine if the target program contains malicious code, none of these references taken either alone or in combination with the prior art of record teach a computer implemented method and a system for identifying malicious code in a target program running in a virtual machine of a computer system specifically including:

i. **Claims 11, 20 and 29**: "automatically configuring a memory map of the virtual machine by assigning areas of the memory map to receive predetermined types of data from the target program based on the file format in order to execute the target program," "constructing the virtual machine from one or more layered operating system shells that correspond with the memory map so that the virtual machine is capable of executing DOS target programs," "setting and resetting behavior flags in a register in order to track behavior of the target program in response to the simulated values, during execution of the target program by the virtual machine," and "storing a sequence in which the behavior flags are set and reset in the register by the target program during execution of the target program by the virtual machine," in combination with the remaining elements and features of the claimed invention.

It is for these reasons that the Applicant's invention defines over the prior art of record.

2. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Russ Guill whose telephone number is 571-272-7955. The examiner can normally be reached on Monday - Friday 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Paul Rodriguez can be reached on 571-272-3753. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application should be directed to the TC2100 Group Receptionist: 571-272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Russ Guill
Examiner
Art Unit 2123

RG

PAUL RODRIGUEZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
7/21/05

PAUL RODRIGUEZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100